IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Applicant(s): Philip D. MacKenzie
Case: 15
Serial No.: 10/600,687
Filing Date: June 20, 2003
Group: 2435
Examiner: Baotran N. To

Title: Methods and Apparatus for Providing Secure Two-Party Public Key Cryptosystem

---

APPEAL BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313

Sir:

Applicant (hereinafter referred to as "Appellant") hereby appeals the final rejection dated June 15, 2009, of claims 1-16 of the above-identified application.

REAL PARTY IN INTEREST

The present application is assigned of record to Lucent Technologies Inc., as evidenced by an assignment recorded June 20, 2003 in the U.S. Patent and Trademark Office at Reel 014224, Frame 0730. On November 30, 2006, the assignee Lucent Technologies Inc. became a wholly-owned subsidiary of Alcatel S.A., which was renamed Alcatel-Lucent. On November 1, 2008, Lucent Technologies Inc. was renamed Alcatel-Lucent USA Inc., which remains a wholly-owned subsidiary of Alcatel-Lucent. Alcatel-Lucent is the real party in interest.

RELATED APPEALS AND INTERFERENCES

There are no known related appeals and interferences.

STATUS OF CLAIMS

The present application was filed on June 20, 2003 with claims 1-16, all of which remain pending. Claims 1, 8, 9 and 16 are the independent claims.

Claims 1-16 stand rejected under 35 U.S.C. §103(a). Claims 1-16 are appealed.

STATUS OF AMENDMENTS

There have been no amendments filed subsequent to the final rejection.

SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 recites a method for use in a device associated with a first party for decrypting a ciphertext according to a Cramer-Shoup based encryption scheme. The method comprises the steps of obtaining the ciphertext in the first party device sent from a device associated with a second party and generating in the first party device a plaintext corresponding to the ciphertext based on assistance from the second party device.

The assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext from the second party device to the first party device. The plaintext represents a result of the decryption according to the Cramer-Shoup based encryption scheme. The first party device and the second party device jointly perform a decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares of a key that each party holds, but neither can decrypt the ciphertext alone.

As described in the specification at, for example, page 4, lines 1-17; page 8, lines 1-9; page 13, lines 18-22; page 15, lines 3-6; and page 21, line 5, to page 22, line 9, an illustrative embodiment includes a method for use in a device (e.g., 202 in FIG. 2) associated with a first party (e.g., alice in FIGS. 1 and 2) for decrypting a ciphertext (e.g., c in FIG. 1) according to a Cramer-Shoup based encryption scheme, the method comprising the steps of obtaining the ciphertext in the first party

device sent from a device (e.g., 204 in FIG. 2) associated with a second party (e.g., bob in FIGS. 1 and 2) and generating (e.g., step 138 in FIG. 1) in the first party device a plaintext (e.g., *w'* in step 140 of FIG. 1) corresponding to the ciphertext based on assistance from the second party device.

As described in the specification at, for example, page 8, lines 1-9; page 14, lines 11-14; and page 14, line 26, to page 15, line 2, the assistance comprises an exchange (e.g, steps 114, 116, 134 and 136 in FIG. 1) of information between the first party device and the second party device separate from the sending of the ciphertext from the second party device to the first party device. As discussed in the specification at, for example, page 15, lines 3-6, the plaintext represents a result of the decryption according to the Cramer-Shoup based encryption scheme. As described in the specification at, for example, page 2, lines 18-21; page 3, lines 18-20; page 4, lines 13-17; page 6, lines 3-10; and page 14, lines 1-10 and 14-23, the first party device and the second party device jointly perform a decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares (e.g., s_1 and s_2) of a key (e.g., s) that each party holds, but neither can decrypt the ciphertext alone.

Claim 8 is directed to a method for use in a device associated with a first party for assisting in decrypting a ciphertext according to a Cramer-Shoup based encryption scheme. The method comprises the steps of receiving a request generated in and transmitted by a second party device for the partial assistance of the first party device in decrypting the ciphertext according to the Cramer-Shoup based encryption scheme and generating results in the first party device based on the partial assistance provided thereby for use in the second party device to complete decryption of the ciphertext.

The assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext from the first party device to the second party device, such that the first party device and the second party device jointly perform a decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares of a key that each party holds, but such that neither can decrypt the ciphertext alone.

As described in the specification at, for example, page 4, lines 1-17; page 8, lines 1-9; page 13, lines 18-23; and page 21, line 5, to page 22, line 9, an illustrative embodiment includes a method

for use in a device (e.g., 204 in FIG. 2) associated with a first party (e.g., bob in FIGS. 1 and 2) for assisting in decrypting a ciphertext (e.g., *c* in FIG. 1) according to a Cramer-Shoup based encryption scheme. As described in the specification at, for example, page 14, line 1, to page 15, line 6, the method comprises steps of receiving a request (e.g., 114 in FIG. 1) generated in and transmitted by a second party device (e.g., 202 in FIG. 2 or "alice" in FIGS. 1 and 2) for the partial assistance of the first party device in decrypting the ciphertext according to the Cramer-Shoup based encryption scheme and generating results (e.g., 134 in FIG. 1) in the first party device based on the partial assistance provided thereby for use in the second party device to complete decryption (e.g., step 138 in FIG. 1) of the ciphertext.

As described in the specification at, for example, page 8, lines 1-9; page 14, lines 11-14; and page 14, line 26, to page 15, line 2, the assistance comprises an exchange (e.g, steps 114, 116, 134 and 136 in FIG. 1) of information between the first party device and the second party device separate from the sending of the ciphertext from the second party device to the first party device. As described in the specification at, for example, page 2, lines 18-21; page 3, lines 18-20; page 4, lines 13-17; page 6, lines 3-10; and page 14, lines 1-10 and 14-23, the first party device and the second party device jointly perform a decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares (e.g., s_1 and s_2) of a key (e.g., *s*) that each party holds, but neither can decrypt the ciphertext alone.

Claim 9 is directed to an apparatus for use in a device associated with a first party for decrypting a ciphertext according to a Cramer-Shoup based encryption scheme. The apparatus comprises a memory and at least one processor coupled to the memory. The at least one processor is operative to obtain the ciphertext in the first party device sent from a device associated with a second party and to generate in the first party device a plaintext corresponding to the ciphertext based on assistance from the second party device.

The assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext from the second party device to the first party device. The plaintext represents a result of the decryption according to the Cramer-Shoup based encryption scheme. The first party device and the second party device jointly perform a

decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares of a key that each party holds, but neither can decrypt the ciphertext alone.

As described in the specification at, for example, page 4, lines 1-17; page 13, lines 18-23; and page 21, line 5, to page 22, line 9, an illustrative embodiment includes an apparatus (e.g., 202 in FIG. 2) for use in a device associated with a first party (e.g., alice in FIGS. 1 and 2) for decrypting a ciphertext (e.g., c in FIG. 1) according to a Cramer-Shoup based encryption scheme. As described in the specification at, for example, page 22, lines 16-26, the apparatus comprises a memory (e.g., 212-A in FIG. 2) and at least one processor (e.g., 210-A in FIG. 2) coupled to the memory. As described in the specification at, for example, page 4, lines 1-17; page 8, lines 1-9; and page 15, lines 3-6, the at least one processor is operative to obtain the ciphertext in the first party device sent from a device associated with a second party and to generate in the first party device a plaintext corresponding to the ciphertext based on assistance from the second party device.

As described in the specification at, for example, page 8, lines 1-9; page 14, lines 11-14; and page 14, line 26, to page 15, line 2, the assistance comprises an exchange (e.g, steps 114, 116, 134 and 136 in FIG. 1) of information between the first party device and the second party device separate from the sending of the ciphertext from the second party device to the first party device. As described in the specification at, for example, page 2, lines 18-21; page 3, lines 18-20; page 4, lines 13-17; page 6, lines 3-10; and page 14, lines 1-10 and 14-23, the first party device and the second party device jointly perform a decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares (e.g., s_1 and s_2) of a key (e.g., s) that each party holds, but neither can decrypt the ciphertext alone.

Claim 16 is directed to an apparatus for use in a device associated with a first party for assisting in decrypting a ciphertext according to a Cramer-Shoup based encryption scheme. The apparatus comprises a memory and at least one processor coupled to the memory. The at least one processor is operative to receive a request generated in and transmitted by a second party device for the partial assistance of the first party device in decrypting the ciphertext according to the Cramer-Shoup based encryption scheme and to generate results in the first party device based on the partial

assistance provided thereby for use in the second party device to complete decryption of the ciphertext.

The assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext from the second party device to the first party device. The plaintext represents a result of the decryption according to the Cramer-Shoup based encryption scheme. The first party device and the second party device jointly perform a decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares of a key that each party holds, but neither can decrypt the ciphertext alone.

As described in the specification at, for example, page 4, lines 1-17; page 13, lines 18-23; and page 21, line 5, to page 22, line 9, an illustrative embodiment includes an apparatus (e.g., 204 in FIG. 2) for use in a device associated with a first party (e.g., bob in FIGS. 1 and 2) for assisting in decrypting a ciphertext (e.g., *c* in FIG. 1) according to a Cramer-Shoup based encryption scheme. As described in the specification at, for example, page 22, lines 16-26, the apparatus comprises a memory (e.g., 212-B in FIG. 2) and at least one processor (e.g., 210-B in FIG. 2) coupled to the memory. As described in the specificaiton, for example, page 14, line 1, to page 15, line 6, the at least one processor is operative to receiving a request (e.g., 114 in FIG. 1) generated in and transmitted by a second party device (e.g., 202 in FIG. 2 or "alice" in FIGS. 1 and 2) for the partial assistance of the first party device in decrypting the ciphertext according to the Cramer-Shoup based encryption scheme and generating results (e.g., 134 in FIG. 1) in the first party device based on the partial assistance provided thereby for use in the second party device to complete decryption (e.g., step 138 in FIG. 1) of the ciphertext.

As described in the specification at, for example, page 2, lines 18-21, illustrative embodiments of the present invention advantageously provide a provably secure protocol for a two-party Cramer-Shoup cryptosystem. See also the specification at, for example, page 5, line 27, to page 6, line 10.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1, 2, 4-6, 8-10, 12-14 and 16 are rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,697,488 (hereinafter "Cramer") in view of U.S. Patent No. 5, 515, 441 (hereinafter "Faucher").

2. Claim 3, 7, 11 and 15 are rejected under 35 U.S.C. §103(a) as being unpatentable over Cramer and Faucher in view of a Cramer et al. article entitled "Multiparty Computation from Threshold Homomorphic Encryption" (hereinafter "Cramer paper").

ARGUMENT

1. Claims 1, 2, 4-6, 8-10, 12-14 and 16 rejected under §103(a) over Cramer and Faucher.

Claims 1, 8, 9 and 16

With regard to the §103(a) rejections, each and every limitation of the independent claims is not met by the collective teachings of Cramer and Faucher. Below, Appellant explains how such portions of Cramer and Faucher fail to teach or suggest each and every limitation. While Appellant may refer from time to time to each reference alone in describing its deficiencies, it is to be understood that such arguments are intended to point out the overall deficiency of the cited combination.

The present Office Action asserts that the previous clarifying limitation added by Appellant in their last response, i.e., "the first party device and the second party device jointly perform a decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares of a key that each party holds," is disclosed by Faucher at column 8, lines 8-55 and Fig. 5. Appellant strongly disagrees with this assertion.

It is to be understood that the claimed invention provides for a jointly performed decryption operation of a given ciphertext. That is, as made clear by the claim language, the first party and the second party each perform one or more subcomputations of the singular decryption operation that results in the decryption of the given ciphertext, and that such subcomputations are based at least in part respective partial shares of a key that each party holds. Thus, neither party can decrypt the given ciphertext alone.

Faucher discloses a completely different protocol. As column 8 and Fig. 5 of Faucher clearly illustrate, while two terminals cooperate in a cryptographic type protocol, the Faucher protocol is a key exchange and not a decryption operation. Also, while there is information exchanged between the two Faucher terminals and decryptions are performed, no where do the two Faucher terminals "jointly perform a decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares of a key that each party holds," as recited in the independent claims. In fact, the entire protocol of column 8 of Faucher is performed in order to generate a session key, which is done by each terminal performing separate decryption operations of certificates received from the other terminal. There is no joint performance of a joint decryption operation whereby each terminal performs subcomputations of the joint decryption operation. Nor is there any disclosure in Faucher that suggests that any such subcomputations are based at least in part respective partial shares of a key that each party holds. In fact, column 8 of Faucher confirms this deficiency by clearly explaining that each terminal decrypts the other's certificate using the KCA public decryption key.

The present Office Action further points to column 2, lines 14-20 of Faucher to assert that here Faucher discloses that the session key that is generated between the first and second parties is used to "decrypt the ciphertext." However, column 2, lines 14-20 of Faucher says no such thing. What is stated there is that the session key agreement protocol of Faucher is capable of preventing the "man-in-the-middle-attack." This is done in the manner disclosed at columns 7 and 8 of Faucher by requiring an authentication process between the first and second parties based on the session key, see column 7, lines 2-23. Since the "man-in-the-middle" cannot generate the session key, he cannot spoof the authentication process between the first and second parties.

Again, Faucher clearly does not disclose that the first party and the second party each perform one or more subcomputations of the singular decryption operation that results in the decryption of the given ciphertext, and that such subcomputations are based at least in part respective partial shares of a key that each party holds. The operations between the first and second parties in Faucher are performed to generate a session key so that each party can be authenticated to the other for any subsequent transfers, not to jointly decrypt the ciphertext.

Cramer fails to remedy theses deficiencies of Faucher. Accordingly, it is believed that the combined teachings of Cramer and Faucher fail to meet the limitations of claim 1.

Also, Appellant maintains that the Examiner has failed to identify a cogent motivation for combining Cramer and Faucher in the manner proposed. Appellant respectfully submits that the conclusory statements made in the final Office Action to support motivation to combine Cramer and Faucher are of the sort rejected by both the Federal Circuit and the U.S. Supreme Court. See KSR v. Teleflex, No. 13-1450, slip. op. at 14 (U.S., Apr. 30, 2007), quoting In re Kahn, 441 F. 3d 977, 988 (Fed. Cir. 2006) ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness."). There has been no showing in the present §103(a) rejection of claim 1 of objective evidence of record that would motivate one skilled in the art to combine Cramer and Faucher to produce the particular limitations in question. The statements of motivation provided by the Examiner appear to be conclusory statements of the type ruled insufficient in KSR v. Teleflex.

For at least these reasons, Appellant asserts that claim 1 is patentable over Cramer and Faucher.

Independent claim 8, 9 and 16 include limitations similar to those of claim 1, and is therefore believed allowable for reasons similar to those described above with reference to claim 1.

Claims 2 and 10

In addition to being allowable for at least the reasons identified above with regard to claims 1 and 9, claims 2 and 10 are also believed to define separately-patentable subject matter over the cited art. More particularly, claims 2 and 10 recite an exchange of information between the first party device and the second party device whereby at least a portion of the information is encrypted using an encryption technique such that one party encrypts information using its own public key and another party can not read the information but can use the information to perform an operation.

The Examiner refers to Cramer at column 7, lines 1-40 and column 9, lines 25-45 as teaching or suggesting the limitations of claims 2 and 10. Although Cramer at column 7, lines 25-26 refers to a public key represented by the numbers g_1, g_2, c, d, and h, the relied-upon portions of Cramer do not

teach or suggest an exchange of information between the first party device and the second party device whereby at least a portion of the information is encrypted using an encryption technique such that one party encrypts information using its own public key and another party cannot read the information but can use the information to perform an operation.

Claims 4 and 12

In addition to being allowable for at least the reasons identified above with regard to claims 1 and 9, dependent claims 4 and 12 are also believed to define separately-patentable subject matter over the cited art. More particularly, claims 4 and 12 recite generating a share of a random secret; generating information representing encryptions of a form of the random secret, a share of a private key, and the ciphertext; transmitting at least the encrypted information to the second party device; and computing the plaintext based at least on the share of the random secret, the share of the private key, the ciphertext, and the data received from the second party device.

The Examiner refers to Cramer at column 7, lines 11-19 as teaching or suggesting the step of generating a share of a random secret. The relied-upon portion of Cramer refers to a private-key choosing step, and does not teach or suggest generating a share of a random secret. Although Cramer, at column 7, lines 10-27 refers to private key Z_q, the relied-upon portions of Cramer do not teach or suggest generating information representing encryptions of a form of the random secret, a share of a private key, and the ciphertext. Furthermore, although Cramer at column 9, lines 25-50 refers to recovering the plaintext m in the decryption step 50, Cramer does not teach or suggest computing the plaintext based at least on the share of the random secret, the share of the private key, the ciphertext, and the data received from the second party device.

Claims 5 and 13

In addition to being allowable for at least the reasons identified above with regard to claims 1 and 9, dependent claims 5 and 13 are also believed to define separately-patentable subject matter over the cited art. More particularly, claims 5 and 13 include limitations wherein the first party device and the second party device additively share components of a private key.

The Examiner refers to Cramer at column 7, lines 10-15 and column 9, lines 35-40 as teaching or suggesting the limitations of claims 5 and 13. However, the relied-upon portions of Cramer do not teach or suggest the recited limitations. Column 7, lines 10-15 of Cramer refers to private-key choosing step 13, and column 9, lines 35-40 refer to decryption of an encryption of a message, which do not teach or suggest the first party device and the second party device additively sharing components of a private key.

Claims 6 and 14

In addition to being allowable for at least the reasons identified above with regard to claims 1 and 9, dependent claims 6 and 14 are also believed to define separately-patentable subject matter over the cited art. More particularly, claims 6 and 14 include limitations directed to generation and exchange of proofs between the first party device and the second party device that serve to verify operations performed by each party.

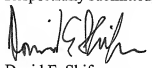
The Examiner refers to Cramer at column 8, line 38 through column 9, line 23, as teaching or suggesting the limitations of claims 6 and 14. However, the relied-upon portion of Cramer refers to verification of ciphertext 30 in verification step 40, which fails to teach or suggest generation and exchange of proofs between the first party device and the second party device that serve to verify operations performed by each party.

2. Claims 3, 7, 11 and 15 rejected under §103(a) over Cramer, Faucher and Faucher paper.

Appellant asserts that the Cramer paper reference fails to remedy the deficiencies described above with regard to Cramer and Faucher. Thus, claims 3, 7, 11 and 15 are patentable at least by virtue of their dependency from claims 1 and 9.

In view of the above, Appellant believes that claims 1-16 are in condition for allowance, and respectfully request reversal of the §103(a) rejections.

Respectfully submitted,



Date: October 14, 2009

David E. Shifren
Attorney for Appellant(s)
Reg. No. 59,329
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-2641

CLAIMS APPENDIX

1. A method for use in a device associated with a first party for decrypting a ciphertext according to a Cramer-Shoup based encryption scheme, the method comprising the steps of:

obtaining the ciphertext in the first party device sent from a device associated with a second party; and

generating in the first party device a plaintext corresponding to the ciphertext based on assistance from the second party device, wherein the assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext from the second party device to the first party device, the plaintext representing a result of the decryption according to the Cramer-Shoup based encryption scheme, such that the first party device and the second party device jointly perform a decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares of a key that each party holds, but such that neither can decrypt the ciphertext alone.

2. The method of claim 1, wherein the generating step further comprises an exchange of information between the first party device and the second party device whereby at least a portion of the information is encrypted using an encryption technique such that one party encrypts information using its own public key and another party can not read the information but can use the information to perform an operation.

3. The method of claim 1, wherein the generating step further comprises an exchange of information between the first party device and the second party device whereby at least a portion of the information is encrypted using an encryption technique having a homomorphic property.

4. The method of claim 1, wherein the generating step further comprises:

generating a share of a random secret;

generating information representing encryptions of a form of the random secret, a share of a private key, and the ciphertext;

transmitting at least the encrypted information to the second party device; and

computing the plaintext based at least on the share of the random secret, the share of the private key, the ciphertext, and the data received from the second party device.

5. The method of claim 1, wherein the first party device and the second party device additively share components of a private key.

6. The method of claim 1, wherein the generating step further comprises generation and exchange of proofs between the first party device and the second party device that serve to verify operations performed by each party.

7. The method of claim 6, wherein the proofs are consistency proofs based on three-move Σ-protocols.

8. A method for use in a device associated with a first party for assisting in decrypting a ciphertext according to a Cramer-Shoup based encryption scheme, the method comprising the steps of:

receiving a request generated in and transmitted by a second party device for the partial assistance of the first party device in decrypting the ciphertext according to the Cramer-Shoup based encryption scheme; and

generating results in the first party device based on the partial assistance provided thereby for use in the second party device to complete decryption of the ciphertext, wherein the assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext from the first party device to the second party device, such that the first party device and the second party device jointly perform a decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares of a key that each party holds, but such that neither can decrypt the ciphertext alone.

9. Apparatus for use in a device associated with a first party for decrypting a ciphertext according to a Cramer-Shoup based encryption scheme, the apparatus comprising:

a memory; and

at least one processor coupled to the memory and operative to: (i) obtain the ciphertext in the first party device sent from a device associated with a second party; and (ii) generate in the first party device a plaintext corresponding to the ciphertext based on assistance from a the second party device, wherein the assistance comprises an exchange of information between the first party device and the

second party device separate from the sending of the ciphertext from the second party device to the first party device, the plaintext representing a result of the decryption according to the Cramer-Shoup based encryption scheme, such that the first party device and the second party device jointly perform a decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares of a key that each party holds, but such that neither can decrypt the ciphertext alone.

10. The apparatus of claim 9, wherein the generating operation further comprises an exchange of information between the first party device and the second party device whereby at least a portion of the information is encrypted using an encryption technique such that one party encrypts information using its own public key and another party can not read the information but can use the information to perform an operation.

11. The apparatus of claim 9, wherein the generating operation further comprises an exchange of information between the first party device and the second party device whereby at least a portion of the information is encrypted using an encryption technique having a homomorphic property.

12. The apparatus of claim 9, wherein the generating operation further comprises: (i) generating a share of a random secret; (ii) generating information representing encryptions of a form of the random secret, a share of a private key, and the ciphertext; (iii) transmitting at least the encrypted information to the second party device; and (iv) computing the plaintext based at least on

the share of the random secret, the share of the private key, the ciphertext, and the data received from the second party device.

13. The apparatus of claim 9, wherein the first party device and the second party device additively share components of a private key.

14. The apparatus of claim 9, wherein the generating operation further comprises generation and exchange of proofs between the first party device and the second party device that serve to verify operations performed by each party.

15. The apparatus of claim 14, wherein the proofs are consistency proofs based on three-move Σ-protocols.

16. Apparatus for use in a device associated with a first party for assisting in decrypting a ciphertext according to a Cramer-Shoup based encryption scheme, the apparatus comprising:

a memory; and

at least one processor coupled to the memory and operative to: (i) receive a request generated in and transmitted by a second party device for the partial assistance of the first party device in decrypting the ciphertext according to the Cramer-Shoup based encryption scheme; and (ii) generate results in the first party device based on the partial assistance provided thereby for use in the second party device to complete decryption of the ciphertext, wherein the assistance comprises an exchange of information between the first party device and the second party device separate from the sending

of the ciphertext from the first party device to the second party device, such that the first party device and the second party device jointly perform a decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares of a key that each party holds, but such that neither can decrypt the ciphertext alone.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.